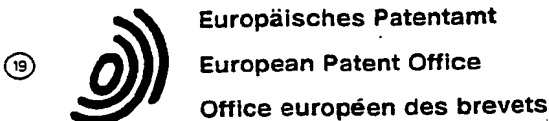


Att.

EP 21360 (7)



①⑪ Publication number:

0 316 689
A2

①⑫

EUROPEAN PATENT APPLICATION

②① Application number: 88118450.1

⑤① Int. Cl.4: **G07F 7/10**

②② Date of filing: 04.11.88

③③ Priority: 13.11.87 JP 288120/87

④③ Date of publication of application:
 24.05.89 Bulletin 89/21

⑧④ Designated Contracting States:
 DE FR GB

⑦① Applicant: **KABUSHIKI KAISHA TOSHIBA**
 72, Horikawa-cho Saiwai-ku
 Kawasaki-shi Kanagawa-ken 210(JP)

⑦② Inventor: **Tamada, Masuo** c/o Patent Division
Kabushiki Kaisha Toshiba 1-1 Shibaura
1-chome
Minato-ku Tokyo 105(JP)
 Inventor: **Matsuoka, Hideo** c/o Patent Division
Kabushiki Kaisha Toshiba 1-1 Shibaura
1-chome
Minato-ku Tokyo 105(JP)
 Inventor: **Tanaka, Tsutomu** c/o Patent Division
Kabushiki Kaisha Toshiba 1-1 Shibaura
1-chome
Minato-ku Tokyo 105(JP)

⑦④ Representative: **Henkel, Feller, Hänzel & Partner**
Möhlstrasse 37
D-8000 München 80(DE)

⑤④ **Portable electronic apparatus.**

⑤⑦ In an IC card having an update function of transaction data, account type, supplementary amount, and valid date are input to the IC card. The IC card adds a renewal number data held therein to the input transaction data, and the data is encrypted using key data, thus generating reference confirmation data. Input confirmation data is generated using the identical encryption generation algorithm by a host system of a credit company. The input confirmation data is supplied to the IC card. A comparison means in the IC card compares the input confirmation data with the generated reference confirmation data. As a result of the comparison, if these data coincide each other, the input data is stored in the memory in the IC card as new transaction data and update processing is executed.

EP 0 316 689 A2

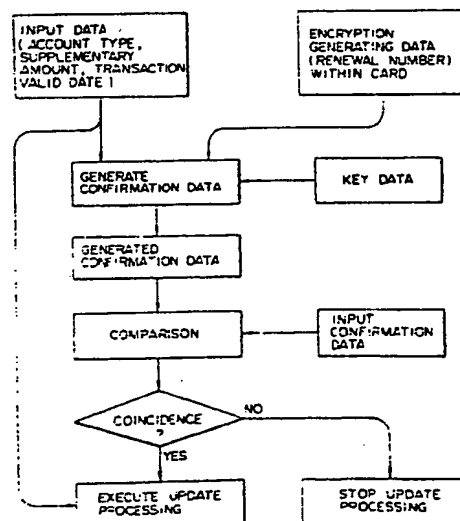


FIG. 3

constituted by, for example, a thin plastic board of rectangular shape. Card main body 1 includes contact section 3, which is electrically connected to integrated circuit (IC) 2 buried in main body 1, for electrically communicating with a terminal device (not shown) in the on-line mode, liquid crystal display section 4 for displaying input/output data, time-related data, and the like, and keyboard 5, all of these units being arranged at predetermined positions on the front surface of main body 1. Card main body 1 additionally contains battery 6 for supplying a power source voltage.

Keyboard 5 includes account keys 7, 8, 9, and 10 for designating an account; numeric keys 11; addition key 12, subtraction key 13, division key 14, and multiplication key 15, these being the four-operation keys; decimal key 16; equal key 17; and the like.

Account key 7 designates a first operation (processing) for a first account (e.g., account data of a first credit company), account key 8 designates a second operation for a second account (e.g., account data of a second credit company), account key 9 designates a third operation for a third account (e.g., account data of a first bank), and account key 10 designates a fourth operation for a fourth account (e.g., account data for a second bank).

Addition key 12 is used as a "next" key for advancing the display state of liquid crystal display section 4, and for mode-selection; subtraction key 13 is used as a "back" key for restoring display section 4 to its previous display state; and equal key 17 serves a dual purpose, being the used as "yes" key and also as the initialization key (power-on key).

Embossed data (not shown) is formed at a predetermined position of the rear surface of card main body 1 as card holder data.

Fig. 2 shows a circuit arrangement of the integrated circuit shown in Fig. 1. Communication control circuit 21, reset control circuit 22, and power source control circuit 23 are connected to contact section 3. In addition, battery check circuit 24 for checking whether the voltage of battery 6 is more than a predetermined value or not is connected to power source control circuit 23. Internal bus 38 is connected to program memory 28 for storing a control program, working memory 29 used for arithmetic operations, data memory 30 consisting of a nonvolatile memory such as an EEPROM for storing transaction data, timer circuit 31 used when time is counted during program execution, and timer circuit section 32 for generating time-piece data including time data and date data. This timer circuit section 32 includes timer circuits 322 and 323, and frequency divider 311. Oscillator 33 having a frequency of 32.768 kHz is

connected to timer circuit section 32.

Display section 4 is connected to internal bus 38 through display control circuit 34 and display driver 35. Keyboard 5 is also connected to internal bus 38 through keyboard interface 36. In addition, confirmation data generating circuit 37 for generating the confirmation data of the input transaction data using key data based on DES (Data Encryption Standard) and CPU (Central Processing Unit) 27 for controlling the entire circuit shown in Fig. 2 are connected to internal bus 38.

Communication control circuit 21 is operated in the on-line mode. More specifically, serial data supplied from the terminal equipment (not shown) through contact section 3 is converted into parallel data and output to data bus 38. Otherwise, parallel data supplied from data bus 38 is converted into serial data and output to the terminal equipment through contact section 3.

Reset control circuit 22 is operated in the on-line mode. This circuit 22 receives a reset signal supplied from the terminal equipment through contact section 3 to initialize CPU 27.

After the predetermined time is elapsed in the on-line mode, power source control circuit 23 is switched to be driven by an external power source (supplied from the terminal equipment through contact section 3) in place of battery 6. In the off-line mode, i.e., when the voltage of the external power source is decreased, power source circuit 23 is switched to be driven by battery 6 in place of the external power source. When key input is not performed (in a stand-by state) in the off-line mode, clock control circuit 25 stops the operation of oscillator 26 for generating a clock having a frequency of 1 MHz. In addition, the clock is not supplied to CPU 27, and the circuit is completely stopped. In this state, when initialization key 17 is turned on, oscillator 26 is operated. In addition, a time-piece clock of 32.768 kHz output from timer circuit section 32 is supplied to CPU 27. When the next key operation is performed after initialization key 17 is turned on, the clock of 1 MHz output from oscillator 26 is supplied to CPU 27. In the on-line mode, by supplying a reset signal from reset control circuit 22, the clock supplied from the terminal equipment through contact section 3 is input to CPU 27.

A transaction function program, a time-piece function program, a calculation function program, an electronic memorandum notebook function program, and the like are stored in program memory 28. CPU 27 selectively executes and processes these programs in program memory 28, so that the transaction function, the time-piece function, the calculation function, the electronic memorandum notebook function, and the like are selectively operated.

Update processing of the transaction limit amount and the transaction valid date of the designated account type as an example of the validity of the input data will be described below with reference to Fig. 3.

The card holder selects the account type by account keys 7 through 10 of keyboard 5. Then, CPU 27 reads out the account data corresponding to the selected account type from data memory 30, displays the account data on liquid crystal display section 4, and displays the message for urging the card holder to input the PIN. When the card holder inputs the PIN by numeric keys 11 of keyboard 5, CPU 27 compares and verifies the input PIN with the PIN in the account data read out from data memory 30 and judges the validity of the card holder. As a result of the judgement, if the card holder is invalid, the message representing the invalidity of the card holder is displayed on liquid crystal display section 4, and the operation is ended. As the result of the above judgement, if the card holder is valid, CPU 27 displays the message "Shopping?" on liquid crystal display section 4. At this time, the card holder repeatedly pushes "next" key 12 of keyboard 5 to select a mode. When the message "Update?" is displayed on liquid crystal display section 4, pushing of "next" key 12 is stopped. When the card holder pushes "yes" key 17 of keyboard 5, CPU 27 sets the update mode, and displays the message for urging the card holder to input the amount on liquid crystal display section 4.

When the card holder, therefore, inputs the supplementary amount of the transaction limit amount to be updated by numeric keys 11 of keyboard 5, CPU 27 displays the message for urging the card holder to input the data on liquid crystal display section 4. The card holder inputs the confirmation data by keyboard 5. The confirmation data input from keyboard 5 is generated as follows. The card holder calls, e.g., a credit company and informs the account type, and the transaction amount and the transaction valid date which are to be updated to the company. As a result, the credit company encrypts a data string of the account type, the transaction amount and transaction valid date to be updated, and the renewal number with key data based on DES, using a host system and the same algorithm as confirmation data generating circuit 37. Then, the confirmation data is generated. The generated confirmation data is informed to the card holder by a phone call. The card holder inputs the confirmation data from keyboard 5.

When the input of the confirmation data is completed as described above, the card holder inputs the account type, and the transaction amount and transaction valid date (year, month,

and day) which are to be updated as the transaction data to be updated. CPU 27 receives these input data and supplies a renewal number (sequence number) in the account data readout from data memory 30 to confirmation data generating circuit 37. Note that the renewal number is updated upon every updating of the transaction limit amount and transaction valid date. Confirmation data generating circuit 37 encrypts the data string of the supplied account type, transaction amount and transaction valid date which are to be updated, and renewal number (stored in the predetermined region of the data memory) using the key data in accordance with DES to generate reference confirmation data. CPU 27 compares the input confirmation data with the reference data. When these data coincide with each other, CPU 27 judges that input data and the input confirmation data are valid, and updates the transaction limit amount data and the transaction valid date data in the selected account data on the basis of the input data. On the other hand, when the above data do not coincide with each other, CPU 27 judges that at least one of the input data and the input personal data is invalid, and stops the update processing.

When the transaction limit amount and the transaction valid date are updated as described above, by inputting the data for updating (account type, supplementary amount, date) from the keyboard, the confirmation data encrypted using the predetermined key data is generated on the basis of the input data and the encryption generating data within the card such as a renewal number stored in the data memory. Then, the generated confirmation data is verified with the confirmation data which is input from the keyboard, and the validity of the above input data is judged. Therefore, the validity of the input data from the keyboard can be judged. When the result of the judgement is negative, the update processing is stopped. Only when the result of the judgement is affirmative, the update processing is executed and the illegal updating of the transaction limit amount data and transaction valid date data which are stored in data memory 30 can be prevented.

When the renewal number (sequence number) is used as the encryption generating data within the card, it can be controlled so that the encryption generating data which was once used cannot be used again. More specifically, the latest renewal number is input with the confirmation data at the next renewal. By comparing the input renewal number with the renewal number in the data memory, when the same or smaller renewal number is input, the update processing can be prohibited.

Note that, although the above-described embodiment is described with reference to the off-line mode, the operation in the on-line mode is similar

12. A portable electronic apparatus characterized by further comprising:
memory means (30) for storing data;
input means (5) for inputting the data;
control means (27, 28) for controlling said memory means and said input means;
confirmation data generating means (37) for generating confirmation data encrypted using predetermined key data on the basis of input data from said input means and inherent data present in said portable electronic apparatus; and
authentication means (27, 28) for verifying the confirmation data, generated by said confirmation data generating means, with the confirmation data input from said input means, to authenticate the validity of the input data.

20

25

30

35

40

45

50

55

7

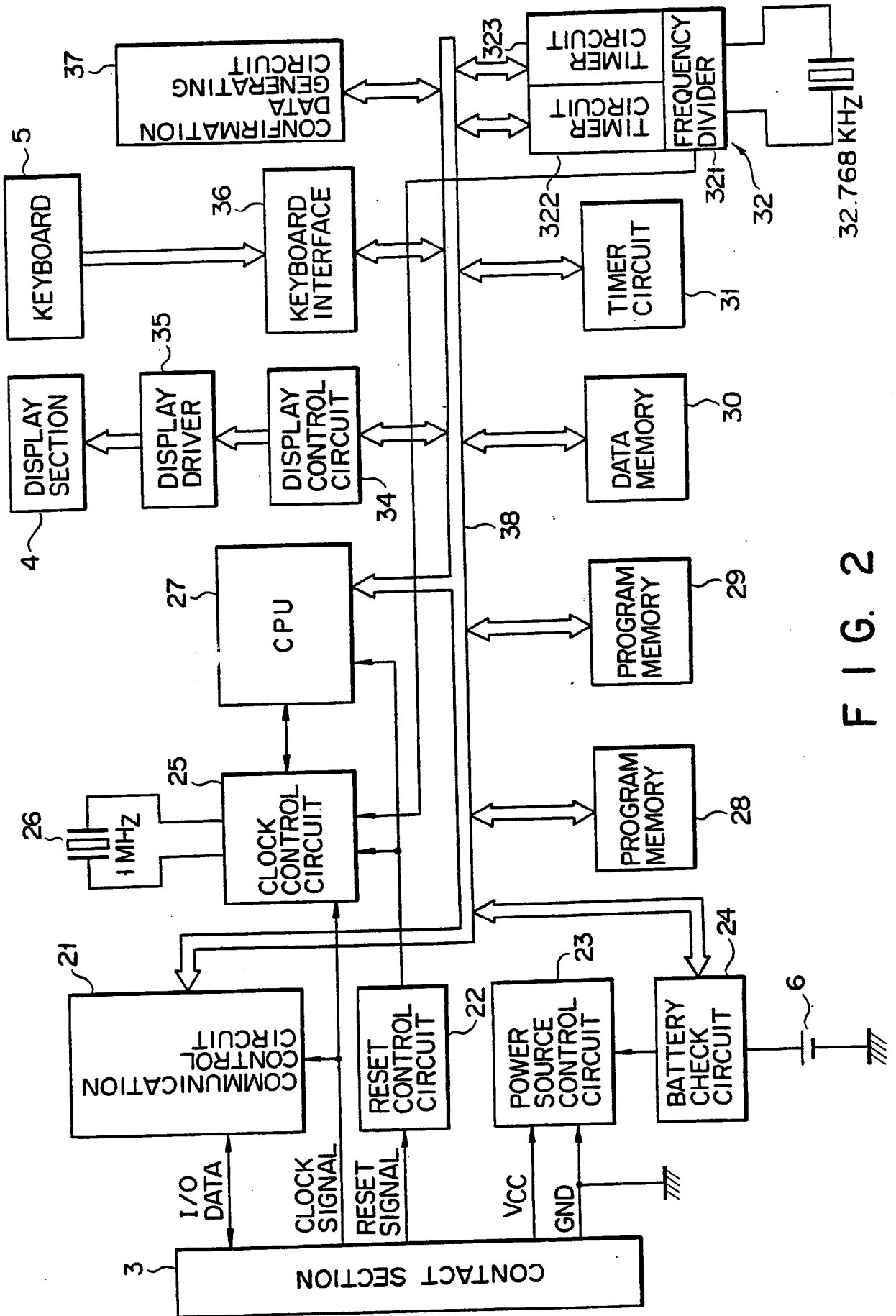


FIG. 2

(19)



Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number:

0 316 689
A3

(12)

EUROPEAN PATENT APPLICATION

(21) Application number: 88118450.1

(51) Int. Cl. 4: G07F 7/10

(22) Date of filing: 04.11.88

(30) Priority: 13.11.87 JP 288120/87

(43) Date of publication of application:
24.05.89 Bulletin 89/21(84) Designated Contracting States:
DE FR GB(68) Date of deferred publication of the search report:
07.02.90 Bulletin 90/06(71) Applicant: **KABUSHIKI KAISHA TOSHIBA**
72, Horikawa-cho Saiwai-ku
Kawasaki-shi Kanagawa-ken 210(JP)(72) Inventor: **Tamada, Masuo** c/o Patent Division
Kabushiki Kaisha Toshiba 1-1 Shibaura
1-chome

Minato-ku Tokyo 105(JP)

Inventor: **Matsuoka, Hideo** c/o Patent Division
Kabushiki Kaisha Toshiba 1-1 Shibaura
1-chome

Minato-ku Tokyo 105(JP)

Inventor: **Tanaka, Tsutomu** c/o Patent Division
Kabushiki Kaisha Toshiba 1-1 Shibaura
1-chome

Minato-ku Tokyo 105(JP)

(74) Representative: **Henkel, Feiler, Hänzeli & Partner**
Möhlstrasse 37
D-8000 München 80(DE)(54) **Portable electronic apparatus.**

(57) In an IC card having an update function of transaction data, account type, supplementary amount, and valid date are input to the IC card. The IC card adds a renewal number data held therein to the input transaction data, and the data is encrypted using key data, thus generating reference confirmation data. Input confirmation data is generated using the identical encryption generation algorithm by a host system of a credit company. The input confirmation data is supplied to the IC card. A comparison means in the IC card compares the input confirmation data with the generated reference confirmation data. As a result of the comparison, if these data coincide each other, the input data is stored in the memory in the IC card as new transaction data and update processing is executed.

EP 0 316 689 A3

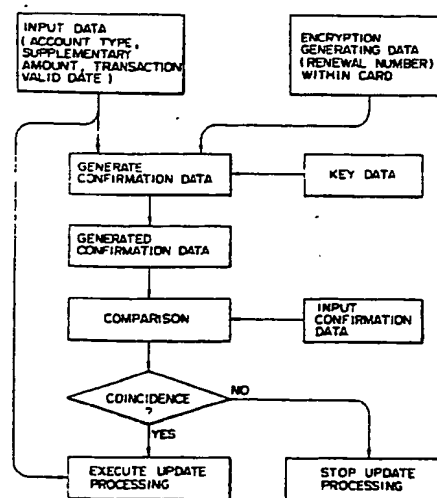


FIG. 3